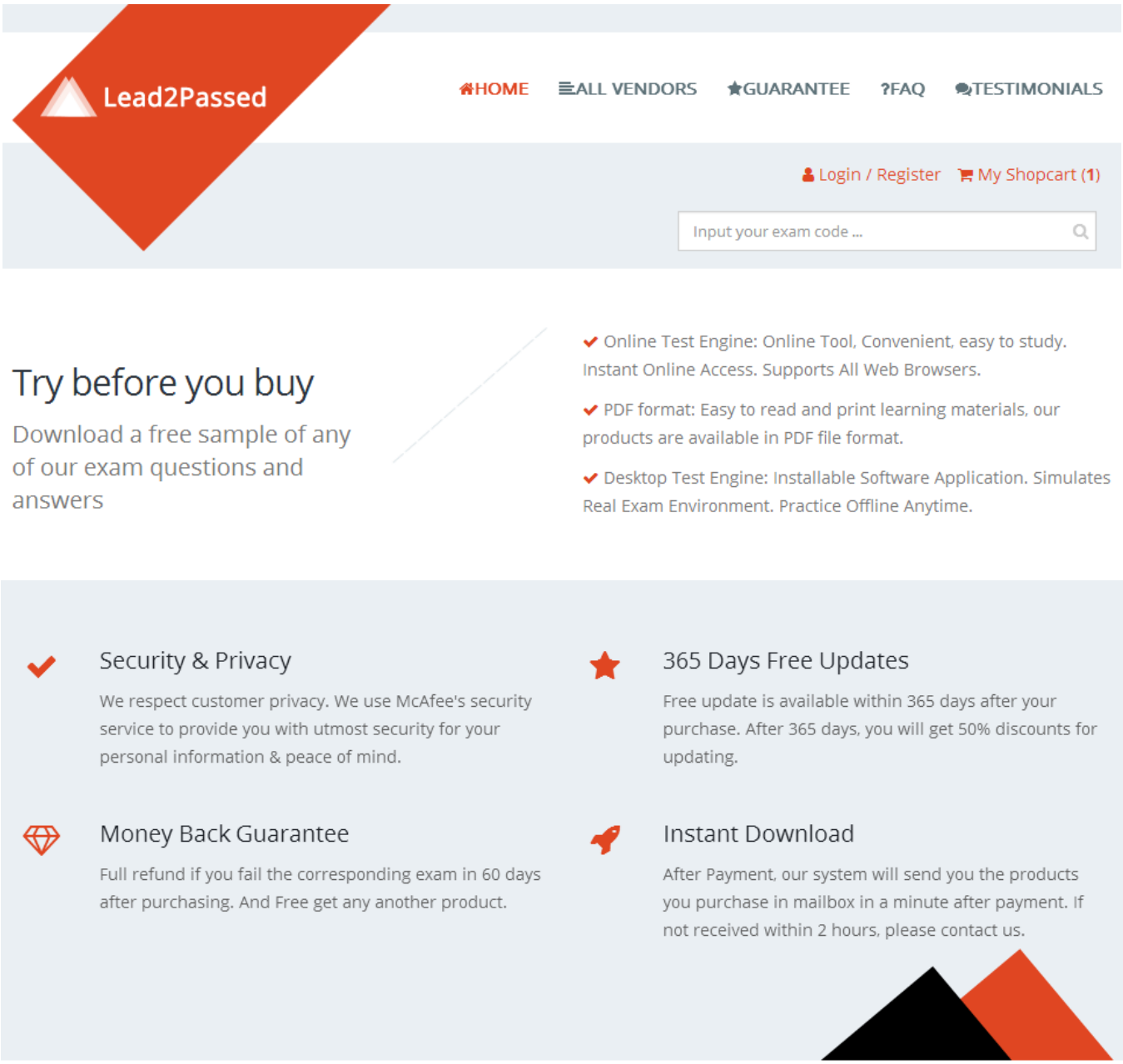
Lead2Passed



http://www.lead2passed.com

Valid Certification Exam Dumps Materials and Study Guide - Lead2Passed

Exam : **RC0-C02**

Title : CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Vendor : CompTIA

Version : DEMO

NO.1 A business wants to start using social media to promote the corporation and to ensure that customers have a good experience with their products. Which of the following security items should the company have in place before implementation? (Select TWO).
A. The company must dedicate specific staff to act as social media representatives of the company.
B. All staff needs to be instructed in the proper use of social media in the work environment.
C. Senior staff biogs should be ghost written by marketing professionals.
D. The finance department must provide a cost benefit analysis for social media.
E. The security policy needs to be reviewed to ensure that social media policy is properly implemented.
F. The company should ensure that the company has sufficient bandwidth to allow for social media traffic.
Answer: A, E

NO.2 A company provides on-demand virtual computing for a sensitive project. The company implements a fully virtualized datacenter and terminal server access with two-factor authentication for access to sensitive data. The security administrator at the company has uncovered a breach in data confidentiality.
Sensitive data was found on a hidden directory within the hypervisor. Which of the following has MOST likely occurred?
A. A stolen two factor token and a memory mapping RAM exploit were used to move data from one virtual guest to an unauthorized similar token.
B. An employee with administrative access to the virtual guests was able to dump the guest memory onto their mapped disk.
C. A host server was left Un-patched and an attacker was able to use a VMEscape attack to gain unauthorized access.
D. A virtual guest was left un-patched and an attacker was able to use a privilege escalation attack to gain unauthorized access.
Answer: C

NO.3 A medical device manufacturer has decided to work with another international organization to develop the software for a new robotic surgical platform to be introduced into hospitals within the next 12 months. In order to ensure a competitor does not become aware, management at the medical device manufacturer has decided to keep it secret until formal contracts are signed. Which of the following documents is MOST likely to contain a description of the initial terms and arrangement and is not legally enforceable?
A. OLA
B. BPA
C. SLA
D. SOA
E. MOU
Answer: E
Explanation:
A memorandum of understanding (MOU) documents conditions and applied terms for outsourcing partner organizations that must share data and information resources. It must be signed by a re presentative from each organization that has the legal authority to sign and are typically secured, as they are considered confidential.
Incorrect Answers:

A: An operating level agreement (O LA) defines the responsibilities of each partner's internal support group and what group and resources are used to meet the specified goal. It is used in conjunction with service level agreements (SLAs).
B: A business partnership security agreement (BPA) is a legally binding document that is designed to provide safeguards and compel certain actions among business partners in relation to specific security-related activities.
C: A service level agreement (SLA) guarantees the level of service the partner is agreeing to provide. It specifies the uptime, response time, and maximum outage time that the partner is agreeing to.
D: Service-orientated architecture (SOA) is a web service that has an abstract architectural style, binding together disjointed pieces of software.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 70, 238

NO.4 A Chief Financial Officer (CFO) has raised concerns with the Chief Information Security Officer (CISO) because money has been spent on IT security infrastructure, but corporate assets are still found to be vulnerable. The business recently funded a patch management product and SOE hardening initiative.
A third party auditor reported findings against the business because some systems were missing patches.
Which of the following statements BEST describes this situation?
A. The CFO is at fault because they are responsible for patching the systems and have already been given patch management and SOE hardening products.
B. The audit findings are invalid because remedial steps have already been applied to patch servers and the remediation takes time to complete.
C. The CISO has not selected the correct controls and the audit findings should be assigned to them instead of the CFO.
D. Security controls are generally never 100% effective and gaps should be explained to stakeholders and managed accordingly.
Answer: D
Explanation:
Security controls can never be run 100% effective and is mainly observed as a risk mitigation strategy thus the gaps should be explained to all stakeholders and managed accordingly.
Incorrect Answers:
A: The CFO's main concern would be of a monetary nature as per the job description and not the IT security infrastructure or patch management per se.
B: The audit findings are not invalid since the audit actually found more missing patches on some systems.
C: The chief information security officer is the executive in the company that has the responsibility over information security in the organization; the CISO does not necessarily select controls.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 204, 213

NO.5 An insurance company has an online quoting system for insurance premiums. It allows potential customers to fill in certain details about their car and obtain a quote. During an investigation, the following patterns were detected:

Pattern 1 - Analysis of the logs identifies that insurance premium forms are being filled in but only single fields are incrementally being updated.
Pattern 2 - For every quote completed, a new customer number is created; due to legacy systems, customer numbers are running out.
Which of the following is the attack type the system is susceptible to, and what is the BEST way to defend against it? (Select TWO).
A. Apply a hidden field that triggers a SIEM alert
B. Cross site scripting attack
C. Resource exhaustion attack
D. Input a blacklist of all known BOT malware IPs into the firewall
E. SQL injection
F. Implement an inline WAF and integrate into SIEM
G. Distributed denial of service
H. Implement firewall rules to block the attacking IP addresses
Answer: C, F
Explanation:
A resource exhaustion attack involves tying up predetermined resources on a system, thereby making the resources unavailable to others.
Implementing an inline WAF would allow for protection from attacks, as well as log and alert admins to what's going on. Integrating in into SIEM allows for logs and other security-related documentation to be collected for analysis.
Incorrect Answers:
A: SIEM technology analyses security alerts generated by network hardware and applications.
B: Cross site scripting attacks occur when malicious scripts are injected into otherwise trusted websites.
D: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.
E: A SQL injection attack occurs when the attacker makes use of a series of malicious SQL queries to directly influence the SQL database.
G: A distributed denial-of-service (DDoS) attack occurs when many compromised systems attack a single target. This results in denial of service for users of the targeted system.
H: Traditional firewalls block or allow traffic. It is not, however, the best way to defend against a resource exhaustion attack.
References:
http://searchsecurity.techtarget.com/feature/Four-questions-to-ask-before-buying-a-Webapplication-firewall
http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM
https://en.wikipedia.org/wiki/Security_information_and_event_management
http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 150, 153

NO.6 A security engineer is responsible for monitoring company applications for known vulnerabilities.
Which of the following is a way to stay current on exploits and information security news?
A. Update company policies and procedures

B. Subscribe to security mailing lists
C. Implement security awareness training
D. Ensure that the organization vulnerability management plan is up-to-date
Answer: B
Explanation:
Subscribing to bug and vulnerability, security mailing lists is a good way of staying abreast and keeping up to date with the latest in those fields.
Incorrect Answers:
A: Updating company policies and procedures are not staying current on the topic since attacks are generated from outside sources and the best way to stay current on what is happening in that particular topic is to subscribe to a mailing list on the topic.
C: Security awareness training serves best as an operational control insofar as mitigating risk is concerned and not to stay current on the topic.
D: Making sure the company vulnerability plan is up to date is essential but will not keep you up to date on the topic as a subscription to a security mailing list.
References:
Conklin, Wm. Arthur, Gregory White and Dwayne Williams, CASP CompTIA Advanced Security Practitioner Certification Study Guide (Exam CAS-001), McGraw-Hill, Columbus, 2012, p. 139
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, p. 219

NO.7 A corporation has expanded for the first time by integrating several newly acquired businesses. Which of the following are the FIRST tasks that the security team should undertake? (Select TWO).
A. Remove acquired companies Internet access.
B. Federate identity management systems.
C. Install firewalls between the businesses.
D. Re-image all end user computers to a standard image.
E. Develop interconnection policy.
F. Conduct a risk analysis of each acquired company's networks.
Answer: E, F

NO.8 A trucking company delivers products all over the country. The executives at the company would like to have better insight into the location of their drivers to ensure the shipments are following secure routes.
Which of the following would BEST help the executives meet this goal?
A. Install GSM tracking on each product for end-to-end delivery visibility.
B. Implement geo-fencing to track products.
C. Require drivers to geo-tag documentation at each delivery location.
D. Equip each truck with an RFID tag for location services.
Answer: B
Explanation:
A Geo-fencing solution would use GPS to track the vehicles and could be configured to inform the executives where the vehicles are.
Geo-fencing is a feature in a software program that uses the global positioning system (GPS) or radio frequency identification (RFID) to define geographical boundaries. A geo-fence is a virtual barrier. Programs that incorporate geo-fencing allow an administrator to set up triggers so when a device enters

(or exits) the boundaries defined by the administrator, a text message or email alert is sent.
Many geo-fencing applications incorporate Google Earth, allowing administrators to define boundaries on top of a satellite view of a specific geographical area. Other applications define boundaries by longitude and latitude or through user-created and Web-based maps.
Incorrect Answers:
A: GSM tracking tracks a mobile phone by detecting the phone's radio signals between radio towers. This solution would require there to be radio towers within range of the phone at all times. This is not always the case when travelling across country. GPS uses satellites which is a better solution.
C: Requiring drivers to geo-tag documentation at each delivery location would provide information when the driver is at a delivery location. However, it would not provide information when the driver is travelling between delivery locations.
D: An RFID tag requires an RFID reader to read the tag. This could work within a building where RFID readers could be installed. However, it is not a practical solution out on the open road as there would be no RFID readers.
References:
http://whatis.techtarget.com/definition/geofencing

NO.9 A security administrator is tasked with increasing the availability of the storage networks while enhancing the performance of existing applications. Which of the following technologies should the administrator implement to meet these goals? (Select TWO).
A. LUN masking
B. Snapshots
C. vSAN
D. Dynamic disk pools
E. Multipath
F. Deduplication
Answer: D, E
Explanation:
We can use dynamic disk pools (DDP) to increase availability and improve performance compared to traditional RAID. Multipathing also improves availability by creating multiple paths to the storage (in case one path fails) and it improves the performance by aggregating the performance of the multiple paths.
DDP dynamically distributes all data, spare capacity, and protection information across a pool of drives.
Effectively, DDP is a new type of RAID level, built on RAID 6. It uses an intelligent algorithm to define where each chunk of data should reside. In traditional RAID, drives are organized into arrays, and logical drives are written across stripes on the physical drives in the array. Hot spares contain no data until a drive fails, leaving that spare capacity stranded and without a purpose. In the event of a drive failure, the data is recreated on the hot spare, significantly impacting the performance of all drives in the array during the rebuild process.
With DDP, each logical drive's data and spare capacity is distributed across all drives in the pool, so all drives contribute to the aggregate 10 of the logical drive, and the spare capacity is available to all logical drives. In the event of a physical drive failure, data is reconstructed throughout the disk pool. Basically, the data that had previously resided on the failed drive is redistributed across all drives in the pool. Recovery from a failed drive may be up to ten times faster than a rebuild in a traditional RAID set, and the performance degradation is much less during the rebuild.

In computer storage, multipath 1/0 is a fault-tolerance and performance-enhancement technique that defines more than one physical path between the CPU in a computer system and its massstorage devices through the buses, controllers, switches, and bridge devices connecting them.
As an example, a SCSI hard disk drive may connect to two SCSI controllers on the same computer, or a disk may connect to two Fibre Channel ports. Should one controller, port or switch fail, the operating system can route the 1/0 through the remaining controller, port or switch transparently and with no changes visible to the applications.
Incorrect Answers:
A: LUN masking is used to control which LUNs are visible to specific servers. It does not improve the availability of the storage networks or the performance of existing applications.
B: A snapshot is a point in time image of the data on a SAN used for backup or recovery purposes. It does not improve the availability of the storage networks or the performance of existing applications.
C: A vSAN is local storage on hypervisor servers combined together to create a "virtual SAN". A vSAN does not improve the availability of the storage networks or the performance of existing applications.
F: Deduplication is the process of eliminating multiple copies of the same data to save storage space. It does not improve the availability of the storage networks or the performance of existing applications.
References:
http://blog.glcomp.com/2013/06/what-is-dynamic-disk-pooling.html
https://en.wikipedia.org/wiki/Multipath_I/0

NO.10 An administrator is tasked with securing several website domains on a web server. The administrator elects to secure www.example.com, mail.example.org, archive.example.com, and www.example.org with the same certificate. Which of the following would allow the administrator to secure those domains with a single issued certificate?
A. Intermediate Root Certificate
B. Wildcard Certificate
C. EV x509 Certificate
D. Subject Alternative Names Certificate
Answer: D
Explanation:
Subject Alternative Names let you protect multiple host names with a single SSL certificate. Subject Alternative Names allow you to specify a list of host names to be protected by a single SSL certificate. When you order the certificate, you will specify one fully qualified domain name in the common name field.
You can then add other names in the Subject Alternative Names field.
Incorrect Answers:
A: An Intermediate Root Certificate is used to trust an intermediate CA (Certification Authority). The Intermediate root CA can issue certificates but the Intermediate Root Certificate itself cannot be used to secure multiple domains on a web server.
B: A wildcard certificate can be used to secure multiple domain names within the same higher level domain. For example: a wildcard certificate "* .example.com" can secure an unlimited number of domains that end in 'example.com' such as domainl.example.com, domain2.example.com etc. A wildcard certificate cannot be used to secure the domains listed in this question.
C: The certificate used to secure the domains will be an x509 certificate but it will not be a standard EV certificate. EV stands for extended validation. With a non-EV certificate, the issuing CA just

ensures that you own the domains that you want to secure. With an EV certificate, further checks are carried out such as checks on your company. EV certificates take longer to issue due to the extra checks but the EV certificate provides extra guarantees to your customers that you are who you say you are. However, a standard EV certificate only secures a single domain.

NO.11 A completely new class of web-based vulnerabilities has been discovered. Claims have been made that all common web-based development frameworks are susceptible to attack. Proof-of-concept details have emerged on the Internet. A security advisor within a company has been asked to provide recommendations on how to respond quickly to these vulnerabilities. Which of the following BEST describes how the security advisor should respond?
A. Assess the reliability of the information source, likelihood of exploitability, and impact to hosted data.
Attempt to exploit via the proof-of-concept code. Consider remediation options.
B. Hire an independent security consulting agency to perform a penetration test of the web servers. Advise management of any 'high' or 'critical' penetration test findings and put forward recommendations for mitigation.
C. Review vulnerability write-ups posted on the Internet. Respond to management with a recommendation to wait until the news has been independently verified by software vendors providing the web application software.
D. Notify all customers about the threat to their hosted data. Bring the web servers down into "maintenance mode" until the vulnerability can be reliably mitigated through a vendor patch.
Answer: A
Explanation:
The first thing you should do is verify the reliability of the claims. From there you can assess the likelihood of the vulnerability affecting your systems. If it is determined that your systems are likely to be affected by the exploit, you need to determine what impact an attack will have on your hosted data. Now that you know what the impact will be, you can test the exploit by using the proof-of concept code. That should help you determine your options for dealing with the threat (remediation) .
Incorrect Answers:
B: While penetration testing your system is a good idea, it is unnecessary to hire an independent security consulting agency to perform a penetration test of the web servers. You know what the vulnerability is so you can test it yourself with the proof-of-concept code.
C: Security response should be proactive. Waiting for the threat to be verified by the software vendor will leave the company vulnerable if the vulnerability is real.
D: Bringing down the web servers would prevent the vulnerability but would also render the system useless. Furthermore, customers would expect a certain level of service and may even have a service level agreement in place with guarantees of uptime.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 375-376

NO.12 ABC Company must achieve compliance for PCI and SOX. Which of the following would BEST allow the organization to achieve compliance and ensure security? (Select THREE).
A. Establish a list of users that must work with each regulation
B. Establish a list of devices that must meet each regulation
C. Centralize management of all devices on the network

D. Compartmentalize the network
E. Establish a company framework
F. Apply technical controls to meet compliance with the regulation
Answer: B, D, F
Explanation:
Payment card industry (PCI) compliance is adherence to a set of specific security standards that were developed to protect card information during and after a financial transaction. PCI compliance is required by all card brands.
There are six main requirements for PCI compliance. The vendor must:
Build and maintain a secure network
Protect cardholder data
Maintain a vulnerability management program
Implement strong access control measures
Regularly monitor and test networks
Maintain an information security policy
To achieve PCI and SOX compliance you should:
Establish a list of devices that must meet each regulation. List all the devices that contain the sensitive data.
Compartmentalize the network. Compartmentalize the devices that contain the sensitive data to form a security boundary.
Apply technical controls to meet compliance with the regulation. Secure the data as required.
Incorrect Answers:
A: It is not necessary to establish a list of users that must work with each regulation. All users should be trained to manage sensitive data. However, PCI and SOX compliance is more about the security of the data on the computers that contain the data.
C: Central management of all devices on the network makes device management easier for administrators. However, it is not a requirement for PCI and SOX compliance.
E: A company framework is typically related to the structure of employee roles and departments. It is not a requirement for PCI and SOX compliance.
References:
http://searchcompliance.techtarget.com/definition/PCI-compliance

NO.13 A company has implemented data retention policies and storage quotas in response to their legal department's requests and the SAN administrator's recommendation. The retention policy states all email data older than 90 days should be eliminated. As there are no technical controls in place, users have been instructed to stick to a storage quota of 500Mb of network storage and 200Mb of email storage. After being presented with an e-discovery request from an opposing legal council, the security administrator discovers that the user in the suit has 1Tb of files and 300Mb of email spanning over two years. Which of the following should the security administrator provide to opposing council?
A. Delete files and email exceeding policy thresholds and turn over the remaining files and email.
B. Delete email over the policy threshold and hand over the remaining emails and all of the files.
C. Provide the 1Tb of files on the network and the 300Mb of email files regardless of age.
D. Provide the first 200Mb of e-mail and the first 500Mb of files as per policy.
Answer: C

NO.14 The Chief Information Security Officer (CISO) at a large organization has been reviewing some

security-related incidents at the organization and comparing them to current industry trends. The desktop security engineer feels that the use of USB storage devices on office computers has contributed to the frequency of security incidents. The CISO knows the acceptable use policy prohibits the use of USB storage devices. Every user receives a popup warning about this policy upon login. The SIEM system produces a report of USB violations on a monthly basis; yet violations continue to occur.
Which of the following preventative controls would MOST effectively mitigate the logical risks associated with the use of USB storage devices?
A. Revise the corporate policy to include possible termination as a result of violations
B. Increase the frequency and distribution of the USB violations report
C. Deploy PKI to add non-repudiation to login sessions so offenders cannot deny the offense
D. Implement group policy objects
Answer: D
Explanation:
A Group Policy Object (GPO) can apply a common group of settings to all computers in Windows domain.
One GPO setting under the Removable Storage Access node is: All removable storage classes: Deny all access.
This setting can be applied to all computers in the network and will disable all USB storage devices on the computers.
Incorrect Answers:
A: Threatening the users with termination for violating the acceptable use policy may deter some users from using USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
B: Increasing the frequency and distribution of the USB violations report may deter some users from using
USB storage devices. However, it is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
C: Offenders not being able to deny the offense will make it easier to prove the offense. However, it does not prevent the offense in the first place and therefore is not the MOST effective solution. Physically disabling the use of USB storage devices would be more effective.
References:
http://prajwaldesai.com/how-to-disable-usb-devices-using-group-policy/

NO.15 The <nameID> element in SAML can be provided in which of the following predefined formats? (Select TWO).
A. X.509 subject name
B. PTR DNS record
C. EV certificate OID extension
D. Kerberos principal name
E. WWN record name
Answer: A, D

NO.16 A security auditor suspects two employees of having devised a scheme to steal money from the company.
While one employee submits purchase orders for personal items, the other employee approves these purchase orders. The auditor has contacted the human resources director with suggestions on how

to detect such illegal activities. Which of the following should the human resource director implement to identify the employees involved in these activities and reduce the risk of this activity occurring in the future?
A. Background checks
B. Job rotation
C. Least privilege
D. Employee termination procedures
Answer: B
Explanation:
Job rotation can reduce fraud or misuse by preventing an individual from having too much control over an area.
Incorrect Answers:
A: To verify that a potential employee has a clean background and that any negative history is exposed prior to employment, a background check is used.
C: The principle of least privilege prevents employees from accessing levels not required to perform their everyday function.
D: The employee termination procedures will not identify the employees involved in these activities and reduce the risk of this activity occurring in the future.
References:
Gregg, Michael, and Billy Haines, CASP CompTIA Advanced Security Practitioner Study Guide, John Wiley & Sons, Indianapolis, 2012, pp. 243, 245, 246